



## **RIMUOVERE IL MALWARE (ADWARE, SPYWARE, VIRUS, TROJAN E WORM)**

**Questa è una guida generica alla rimozione del malware, compresi adware – spyware - virus - trojan e worm** (ormai, la loro definizione è molto difficile, giacché questo malware spesso è un po' l'uno e un po' l'altro).

Questa guida non è da considerarsi come un semplice “collage” tra diverse tipologie di interventi a seconda del tipo di adware – spyware – virus – trojan e worm, ma comprende semplicemente delle linee-guida di intervento, ad uso di un utente che ha un minimo di volontà e dimestichezza con il proprio S.O., ma che è alle prese con una rimozione che si rivela particolarmente complicata.

Qualunque intervento apportiate al vostro p.c., anche se in base alle indicazioni di questa guida, è a VOSTRO rischio e pertanto non ci potete imputare nessuna responsabilità in merito.

Non è detto, infine, che dobbiate per forza seguire la guida punto per punto: ripetiamo che queste sono solo indicazioni generiche di intervento.

Prima di procedere, assicurarsi **SEMPRE** che ci sia un firewall attivato nel proprio computer.

Se il proprio computer è già stato infettato, l'attivazione del firewall limiterà gli effetti del malware sul computer.

Come abilitare l'Internet Connection Firewall (ICF) in Windows XP (se non si ha un altro firewall più sicuro).

- 1) Fare clic su “Start” e poi su “Pannello di controllo”.
- 2) Fare clic su “Connessioni di rete”.
- 3) Fare clic con il tasto destro del mouse sulla connessione che si utilizza per connettersi a Internet (Dial-up, LAN, o High-Speed Internet) e poi fare clic su “Proprietà”.
- 4) Nel tab “Avanzate”, in “Firewall connessione Internet”, selezionare “Proteggi il mio computer e la rete limitando o impedendo l'accesso al computer da Internet” e poi fai clic su “OK”.
- 5) Il firewall di Windows XP è ora abilitato.

**Attenzione:** ci sono in giro programmi che eliminano gli spyware, ma a loro volta installano uno spyware nascosto e disabilitano gli spyware “buoni”!

Un esempio di falsi anti-spyware: SpyBan, SpyWiper.

Installate solo i programmi più seri e più conosciuti!

Ugualmente, tra i processi attivi che potrete trovare nel Task Manager vi sono dei programmi con nomi simili a quelli innocui.

Esempio: "svchosts.exe" è la versione fasulla di "svchost.exe", cioè è un virus il cui processo imita il nome di un servizio "buono" per passare inosservato, oppure "iexplorer.exe" fa il verso a "iexplore.exe", ma capita anche di trovare uno "Spybot.exe" che fa il verso a "SpybotSD.exe", oppure un apparentemente innocuo "launcher.exe" o "iedriver.exe", oppure un insidioso "microsoft.exe" o "cmd32.exe"!

## A) COSA FARE PRIMA DELLA RIMOZIONE

1) **La prima cosa da fare:** abilitare la visualizzazione delle cartelle e dei file nascosti dal menu "Strumenti / Opzioni cartella / Visualizzazione" di Windows (il percorso può leggermente variare a seconda della versione del Sistema operativo) ed anche deselezionare le due caselle "Nascondi i file protetti e di sistema (consigliato)" e deselezionare "Nascondi le estensioni dei file per i tipi conosciuti".

In questo modo, anche il malware più "invisibile" dovrebbe essere individuato dall'Explorer (non Internet Explorer, ma l'Esplora Risorse di Windows), che non è uno strumento efficace.

2) **Utilizzare Internet:** se il nostro antivirus o antispyware (è aggiornato, vero? Fate quotidianamente la scansione delle vostre unità dopo l'aggiornamento, vero?) ha rilevato un malware che NON ci impedisce il collegamento ad Internet, collegatevi ad Internet per:

- aggiornare ed utilizzare SPESSO la funzione Windows Update per ottimizzare il vostro sistema operativo (anche se alcuni tipi di virus, come Blaster, fanno cadere la connessione ad Internet dopo circa 60 secondi...);
- trovare le maggiori informazioni possibili sul "nemico", tramite un motore di ricerca (esempio: [www.google.it](http://www.google.it) ), grazie ad articoli, forum e bollettini di sicurezza;
- trovare uno specifico programma di rimozione per quel determinato virus ("removal tool"), molto spesso Microsoft - oppure le grandi case produttrici di antivirus - rilasciano un programma gratuito di rimozione;
- scaricare l'ultima versione del proprio antivirus o del proprio antispyware, oppure scaricare gli ultimi aggiornamenti degli stessi;
- scaricare alcuni programmi freeware che vi aiuteranno a prevenire o combattere o curare il malware:
- scaricare il programma (non indispensabile) HijackThis (<http://216.180.233.163/~merijn/files/HijackThis.exe> ) anche se non siete infetti, in modo di prendere visione dei processi e dei vari settaggi del registro del vostro p.c.;
- scaricare il programma (non indispensabile) Autoruns dal sito <http://www.sysinternals.com/ntw2k/freeware/autoruns.shtml> ; questa applicazione non si installa e mostra i programmi configurati per

essere eseguiti durante il boot o il login del sistema, nell'ordine in cui Windows li esegue. Tali programmi includono quelli nella cartella Esecuzione Automatica, i Servizi, e quelli contenuti come valori nelle chiavi di registro di Run, RunOnce, ed altre;

- scaricare il programma (indispensabile) RegSeeker dal sito <http://www.hoverdesk.net/freeware.htm> ; questa applicazione non si installa e mostra eventuali chiavi di registro non rimosse manualmente, ripulendolo dalle anomalie ed eliminando facilmente tutte le tracce lasciate dai programmi disinstallati come file .DLL, settaggi nel Registro di Sistema, tipi di file associati, altre funzioni contenute nello stesso Autoruns come la visualizzazione dei programmi che si caricano all'avvio: il computer – anche se non siete infetti – funzionerà comunque meglio;
- scaricare i programmi PDfind, StartMenuCleaner, WinRAR (a questo indirizzo e' presente anche la versione 3.51 in Italiano: <http://www.winrar.it/prelievo.php4?url=prelievo/WRar351it.exe> ) o Nero; non sono indispensabili, ma il loro file manager è molto più efficiente dell'Esplora risorse di Windows;
- scaricare i programmi (indispensabili) Firefox e Thunderbird dalla sezione "Download" di [www.mozillaitalia.org](http://www.mozillaitalia.org) ; vi serviranno ad installare due programmi più sicuri e più seri rispetto all'Internet Explorer o all'Outlook Express con il quale vi siete infettati.

E se non potete collegarvi ad Internet?

Fatevi scaricare i suddetti programmi da un amico.

Alcuni indirizzi utili, ma attenti perché non sono sempre aggiornatissimi (si ringrazia [www.wintricks.it](http://www.wintricks.it) ):

<b>Categoria: (F=Freeware)</b>	<b>Cosa fa:</b>	<b>Scan on- line:</b>	<b>Download:</b>
<b><u>Anti-Spyware:</u></b> <b><u>Ad-aware (F)</u></b>	Rimuove, immunizza e protegge da ulteriori tentativi di intrusione. In italiano		<b><u>Download:</u></b> <b><u>aggiorna</u></b>
<b><u>Ewido</u></b>	Rimuove, immunizza e protegge da ulteriori tentativi di intrusione	<b><u>Free</u></b>	<b><u>Scarica</u></b>
<b><u>PestPatrol</u></b>	Rimuove, immunizza e protegge da ulteriori tentativi di intrusione	<b><u>Scan</u></b> <b><u>on- line</u></b> <b><u>(beta)</u></b>	<b><u>Pre- Scan</u></b> <b><u>on- line</u></b> <b><u>automatico</u></b>
<b><u>PestScan</u></b>	Scansione on-line del PC alla ricerca di spyware, dialers, trojan e virus	<b><u>Scan</u></b> <b><u>on- line</u></b>	<b><u>aggiorna</u></b>
<b><u>Spybot - Search &amp; Destr. (F)</u></b>	Rimuove, immunizza e protegge da ulteriori tentativi di intrusione, blocco del file HOSTS e della pagina iniziale. In italiano.		<b><u>aggiorna</u></b>
<b><u>SpyChecker</u></b>	Rimuove, immunizza e protegge da ulteriori tentativi di intrusione, blocco del file HOSTS e della pagina iniziale		
<b><u>Spy Sweeper</u></b>	Rimuove, immunizza e protegge da ulteriori tentativi di	<b><u>Free</u></b>	<b><u>Scarica</u></b>

<p><b><u>Spyware Blaster</u></b></p>	<p>intrusione</p> <p>Rimuove, immunizza e protegge da ulteriori tentativi di intrusione, blocco del file HOSTS e della pagina iniziale</p>	<p><b><u>Scan on-line</u></b></p>	
<p><b><u>Spyware Terminator</u></b> <b><u>Trend Micro</u></b> <b><u>Antispyware (F)</u></b></p>	<p>Ex CWSredder. Utility specializzata per rimuovere CoolWebSearch, la cui totale rimozione è particolarmente difficile</p>	<p><b><u>Free Scan on-line</u></b></p>	<p><b><u>Scarica</u></b> <b><u>Scarica</u></b></p>
<p><b><u>Antivirus:</u></b> <b><u>Aladdin eSafe Desktop</u></b> <b><u>AntiVir Personal Edition</u></b> <b><u>AntiVirusKit</u></b> <b><u>Avast! antivirus (F)</u></b> <b><u>AVG Anti-Virus (F)</u></b> <b><u>BitDefender</u></b></p>	<p>In italiano</p> <p>Scansione on-line del PC alla ricerca di spyware, dialers, trojan e virus</p>	<p><b><u>Scan on-line</u></b></p>	<p><b><u>aggiorna</u></b> <b><u>automatico</u></b> <b><u>Trial</u></b> <b><u>aggiorna</u></b> <b><u>aggiorna giornaliero</u></b></p>
<p><b><u>Dr.Web</u></b></p>		<p><b><u>Scan on-line</u></b> <b><u>Scan on-line (files)</u></b></p>	<p><b><u>aggiorna</u></b></p>
<p><b><u>eTrust InoculateIT</u></b> <b><u>F-Prot Antivirus</u></b> <b><u>F-Secure Anti-Virus</u></b> <b><u>Kaspersky Anti-Virus (AVP)</u></b></p>		<p><b><u>Scan on-line (files)</u></b></p>	<p><b><u>aggiorna</u></b> <b><u>aggiorna</u></b> <b><u>aggiorna</u></b> <b><u>giornaliero</u></b></p>
<p><b><u>McAfee VirusScan</u></b></p>		<p><b><u>Scan on-line</u></b></p>	<p><b><u>aggiorna</u></b></p>
<p><b><u>NOD32 Antivirus System</u></b> <b><u>Norton AntiVirus</u></b></p>		<p><b><u>Scan on-line</u></b></p>	<p><b><u>aggiorna</u></b> <b><u>aggiorna</u></b></p>
<p><b><u>Online Malware Scanner</u></b> <b><u>Panda Antivirus</u></b></p>	<p>Multi AV Scanner - abilitare JavaScript</p> <p>Scansione on-line del PC alla ricerca di spyware, dialers, trojan e virus</p>	<p><b><u>Scan on-line</u></b></p>	<p><b><u>aggiorna</u></b> <b><u>automatico</u></b></p>
<p><b><u>PC-Cillin</u></b></p>		<p><b><u>Scan on-line</u></b></p>	<p><b><u>aggiorna</u></b></p>
<p><b><u>RAV Antivirus</u></b></p>			<p><b><u>aggiorna</u></b></p>

<p><b>Sophos Anti-Virus</b> <b><u>The Cleaner</u></b> <b><u>Virus Total</u></b></p>	<p>Trojan remover</p> <p>Controllo on-line con 18 diversi antivirus di un file dell'utente di massimo 5 MB. È utile per identificare il malware (anche se ogni antivirus da un proprio nome al "nemico"), ma non rimuove quanto rilevato. Multi AV Scanner - abilitare JavaScript</p>	<p><b>Scan on-line</b></p>	<p><b><u>aggiorna</u></b> <b><u>aggiorna</u></b></p>
<p><b><u>Browser:</u></b> <b><u>Firefox (F)</u></b> <b><u>SeaMonkey (F)</u></b></p>	<p>Browser più sicuro di Internet Explorer. In italiano</p> <p>Ex Mozilla Suite. E' una suite di programmi (browser, client e-mail, composer...) più sicura di Internet Explorer ed Outlook. In italiano</p>		<p><b><u>Download:</u></b> <b><u>Scarica</u></b> <b><u>Scarica</u></b></p>
<p><b><u>Client posta elettron.:</u></b> <b><u>ThunderBird (F)</u></b></p>	<p>Client di posta più sicuro di Outlook o Outlook Express. In italiano</p>	<p><b><u>Download:</u></b> <b><u>Scarica</u></b></p>	
<p><b><u>Firewall:</u></b> <b><u>Black ICE Pc Protection</u></b> <b><u>Jetico Personal Firewall</u></b> <b><u>Kerio Personal firewall</u></b> <b><u>Look'n'stop Personal firewall</u></b> <b><u>Norton Personal firewall</u></b> <b><u>Outpost Firewall</u></b> <b><u>Sygate Personal firewall</u></b> <b><u>Tiny Personal firewall</u></b> <b><u>Zone Alarm firewall (F)</u></b> <b><u>Siti riguardanti la Sicurezza:</u></b> <b><u>AuditmMyPC.com</u></b></p>	<p>In italiano</p>	<p><b><u>Download:</u></b> <b><u>Demo</u></b></p> <p><b><u>Free</u></b></p> <p><b><u>Scarica</u></b></p> <p><b><u>Trial</u></b></p> <p><b><u>Trial</u></b></p> <p><b><u>Pro – Free Trial Pro – Free Trial Pro</u></b></p> <p><b><u>Free – Plus – Pro</u></b> <b><u>Test online:</u></b> <b><u>Scan on-line</u></b> <b><u>Test on-line</u></b></p>	
<p><b><u>Browser Challenger</u></b> <b><u>Browser Security Test</u></b></p>	<p>Test sulla sicurezza del vostro browser. Sito di Paolo Attivissimo. In italiano</p> <p>Test sulla sicurezza del vostro browser. In inglese</p>	<p><b><u>Scan on-line</u></b> <b><u>Advisory</u></b></p>	
<p><b><u>CERT Difesa Browser Spy</u></b> <b><u>Gibson Research Corporation</u></b> <b><u>Guninski</u></b> <b><u>Microsoft Security Bulletin</u></b></p>	<p>Test sulla sicurezza del vostro browser. In inglese</p> <p>Disabilitazione di servizi critici per la sicurezza. Tra i tools: Un'PNP, DComb, ShotMess. Sito molto imparziale</p> <p>Test sulla sicurezza del vostro browser. In inglese</p> <p>In Italiano. Gli ultimi bollettini</p>	<p><b><u>ShieldsUP!</u></b></p>	
<p><b><u>Microsoft Security Guidance Center.</u></b> <b><u>PopUp Test</u></b> <b><u>PC Flank</u></b></p>	<p>In italiano</p> <p>Test sul blocco dei pop up del vostro browser. In inglese. Poco attendibile perché considera pop up anche dei menù di scrollino</p> <p>Test sulla sicurezza del vostro browser. In inglese. Poco</p>	<p><b><u>Scan on-</u></b></p>	

<p><u><a href="#">Qualys Browser Check Salvatore Aranzulla's Lab Secunia</a></u></p>	<p>attendibile, perché consiglia sempre determinati software a pagamento, paventando minacce anche inesistenti Test sulla sicurezza del vostro browser. In inglese</p>		<p><u><a href="#">line</a></u></p>
<p><u><a href="#">Sygate Online Services Symantec Security Check The Proxy connection TrojanScan.com</a></u></p>	<p>Test sulla sicurezza del vostro browser. In italiano</p> <p>Offre gli elenchi delle falle ancora aperte e le relative dimostrazioni su tutti i browser. Test sulla sicurezza del vostro browser. In inglese</p>		<p><u><a href="#">Scan on-line</a></u> <u><a href="#">Scan on-line</a></u> <u><a href="#">Scan on-line</a></u> <u><a href="#">Scan on-line</a></u> <u><a href="#">Scan on-line</a></u> <u><a href="#">Scan on-line</a></u> <u><a href="#">Scan on-line</a></u></p>
<p><u><a href="#">Winzozz</a></u></p>	<p>Sito molto completo e vario sulla sicurezza. In italiano</p>		<p><u><a href="#">Varie</a></u></p>
<p><b>Tools di rimozione:</b> <u><a href="#">Avast Cleaner (F)</a></u> <u><a href="#">Bit Defender Removal Tools HijackThis (F)</a></u></p>	<p>Tools "rapido" per la rimozione dei virus più diffusi</p> <p>Ricerca le potenziali voci che possono essere l'obiettivo di programmi dannosi come BOH's, toolbar, ActiveX, programmi sospetti caricati all'avvio o pagine iniziali o di ricerca reindirizzate</p>		<p><b>Download:</b></p> <p><u><a href="#">Scarica</a></u> <u><a href="#">Scarica</a></u></p>
<p><u><a href="#">Kaspersky Removal Tools Microsoft Strumento rimozione malware Norton Removal Tools Stinger (F)</a></u></p>	<p>Tools "rapido" per la rimozione dei virus più diffusi</p>		<p><u><a href="#">Scarica</a></u> <u><a href="#">Scarica</a></u> <u><a href="#">Scarica</a></u></p>
<p><b>Vari:</b> <u><a href="#">ProceXP (ProcExplorer) Safe XP StartMenuCleaner Windows Worms Doors Cleaner (WWDC)</a></u></p>	<p>Visualizzatore di processi, molto potente</p> <p>Attenzione: Safe XP interviene sulle aree portanti del sistema, l'uso senza cognizione di causa può portare a malfunzionamenti Nel menù Avvio e nella barra Avvio veloce, in cui spesso si inseriscono direttamente copie degli eseguibili e non i link, si rimuovono velocemente tutti i link non validi. Attenzione: i possessori del firewall Sygate Pro potrebbero incappare in un problema di corruzione risolvibile qui : <u><a href="http://forums.sygate.com/vb/showthread.php?s=&amp;threadid=1934">http://forums.sygate.com/vb/showthread.php?s=&amp;threadid=1934</a></u></p>		<p><u><a href="#">Scarica</a></u></p>

3) Fate una copia di tutto il vostro Registro di Sistema:

- "Start / Esegui..." e digitare "regedit" senza virgolette, poi dare l'invio con il tasto "Ok";
- Da "Registro di configurazione" scegliere "Esporta file dal Registro di configurazione";

- In "Intervallo di esportazione" selezionare "Tutto", dare un nome al salvataggio e posizionarlo in una cartella di backup;
  - questa copia, sicuramente infetta e possibilmente da "zippare" con password (in modo da evitare che possa essere utilizzata da altri utenti del vostro p.c.) , vi servirà – però – in caso di grossi malfunzionamenti dovuti alla erronea cancellazione di chiavi di registro indispensabili;
- 4) Controllare poi, tramite il comando "Start / Esegui../ msconfig" che le varie linguette (soprattutto "Esecuzione automatica") non presentino un'applicazione denominata "MSBLASTER.EXE" o altro nome "sospetto" o "sconosciuto". In caso esso ci sia, togliere il segno di spunta da tale applicazione.
- 5) Disattivate il "Ripristino Configurazione di Sistema" (la descrizione che segue varia a seconda della versione del Sistema Operativo):
- Dal "Desktop" selezionare l'icona "Risorse del Computer" tramite il tasto destro del mouse;
  - Selezionare l'opzione "Proprietà";
  - Posizionarsi sulla cartella "Ripristino Configurazione di Sistema";
  - Inserire il segno di spunta nella casella "Disattiva Ripristino Configurazione di Sistema";
  - Selezionare l'opzione "Applica" posta in basso a destra della finestra;
  - Chiudere la finestra tramite il proprio pulsante di chiusura contrassegnato da una "X" posizionato in alto a destra;
- 6) Cancellate tutte le voci sospette che sono presenti nel menu "Start / Programmi / Esecuzione automatica".
- 7) Controllate anche la barra dell'Avvio veloce, in cui spesso si inseriscono direttamente copie degli eseguibili e non i collegamenti (link). Poi con StartMenuCleaner (o programma simile, o a mano) rimuovete velocemente tutti i link non validi.
- 8) Controllate anche se, nel Pannello di Controllo, appare qualche connessione diversa dalla vostra abituale (chiaro sintomo di un dialer installato): cancellatela senza timori, anche se è diventata quella "predefinita".
- 9) Controllate il file WIN.INI.  
Il file WIN.INI si trova in C:\Windows (Win9x/Me/XP) o C:\Winnt (WinNT/2000) ed è visibile se viene abilitata l'opzione "Visualizza file e cartelle nascoste" in Risorse del computer / Strumenti / Opzioni Cartella e poi la scheda "Visualizzazione". Questo file viene eseguito all'avvio di Windows.  
Fatene una copia di sicurezza prima di metterci le mani dentro!  
Non è assolutamente facile comprendere cosa è malware e cosa non lo è in questo file.  
Alcuni validi programmi e molti virus vengono caricati all'avvio grazie a questo metodo nella sezione [windows] grazie al comando "Esegui=" o "load=" nel modo seguente:
- ```
[windows]
run=hpfsched
run=%Windows%\CapsideRed.pif
load=asistat.exe
```

**Load = "C:\Windows\System32.exe"**

Nel primo esempio (prima riga), "hpfsched" sta ad indicare di effettuare la pulizia delle cartucce nella stampante HP DeskJet di tanto in tanto per mantenere una qualità di stampa elevata. Può essere rimosso dalla riga Run del file win.ini, se non si vuole questa opzione.

Nel secondo esempio (seconda riga), "CapsideRed.pif" è stato aggiunto dal virus Caspid ed ovviamente è da rimuovere (con %Windows% s'intende C:\Windows o C:\Winnt).

Nel terzo esempio (terza riga), "asistat.exe" carica l'eseguibile che monitorizza la stampante NEC SuperScript printer. Può essere rimosso dalla riga load del file win.ini, se non si vuole questa opzione.

Nell'esempio finale, (ultima riga) "System32.exe" è stato aggiunto dal virus Mari ed ovviamente è da rimuovere.

#### **10) Controllate il file SYSTEM.INI.**

Il file SYSTEM.INI si trova in C:\Windows (Win9x/Me/XP) or C:\Winnt (WinNT/2000) ed è visibile se viene abilitata l'opzione "Visualizza file e cartelle nascoste" in Risorse del computer -> Strumenti -> Opzioni Cartella e poi la scheda "Visualizzazione". Questo file viene eseguito all'avvio di Windows.

Fatene una copia di sicurezza prima di metterci le mani dentro!

A differenza del file visto in precedenza, l'unica voce valida nella riga "shell=" è:

```
[boot]
shell=Explorer.exe
```

Ad ogni modo, alcuni virus usano questa riga per essere eseguiti all'avvio. Ad esempio:

```
[boot]
shell=Explorer.exe %Windows%\Capside.exe
```

La stringa "%Windows%\Capside.exe" è stata aggiunta dal virus Caspid ed ovviamente è da rimuovere (con %Windows% s'intende C:\Windows o C:\Winnt).

#### **11) Controllate il file IERESSET.INF.**

Nella cartella (nascosta) C:\WINDOWS\INF è presente un file denominato IERESSET.INF che può essere utilizzato da Internet Explorer per ripristinare le impostazioni di configurazione scelte al momento dell'installazione di Windows. Alcuni malware modificano il file IERESSET.INF in modo tale che, qualora si tenti un ripristino delle impostazioni iniziali del browser, Internet Explorer si configurerà di nuovo con i parametri scelti dal malware. Se non siete sicuri della genuinità di tale file, fatevi prestare una copia dello stesso da un vostro amico che ha il sistema operativo simile al vostro e utilizzate tale copia per sostituire il vostro IERESSET.INF. Simili interventi sono catalogati da HijackThis nel gruppo 014.

## **B) COSA FARE DURANTE LA RIMOZIONE**

12) Avviate l'antivirus o l'antispymware aggiornato e scansionate nuovamente le vostre unità non removibili.

13) Se l'antivirus o l'antispymware trova un malware, il comportamento è leggermente differente da programma a programma e da malware a malware.

Si può lasciare fare tutto al proprio antivirus o antispymware, selezionando le sue apposite opzioni, oppure ANCHE scovare e rimuovere manualmente il virus – worm – trojan.

Ad esempio, con il famigerato W.32.Blaster.Worm, accade che se il computer si riavvia ripetutamente, bisogna disconnettersi da Internet prima di abilitare il firewall.

Per disconnettere il computer da Internet:

*Utenti con connessione a banda larga:* scollegare il cavo di rete/telefonico dal modem o dalla presa del telefono.

*Utenti con connessione "Dial-up" (modem analogico):* scollegare il cavo telefonico dal modem o dalla presa del telefono.

14) Svuotare il Cestino di Windows.

15) Poi svuotare i file temporanei di Internet, covo sempre ricco di "pirati".

Potete usare l'utilità del "Pannello di controllo / Opzioni Internet / File temporanei Internet / Elimina cookie... / Elimina file...", ma non ripulisce tutto, anche l'Esplora Risorse di Windows – come detto – non è uno strumento efficace.

16) Degli ottimi file manager sono quelli di WinRAR oppure Total Commander, ma anche con Nero (sì, proprio il programma di masterizzazione) è possibile vedere file che risultano "invisibili" all'Esplora Risorse di Windows.

17) Poi controllate da "Start / Programmi / Accessori / Utilità di sistema / Pulitura disco" che non ci siano file sospetti: eventualmente, cancellare tutto!

18) Poi cancellate i temporanei "C:\Windows\Temp".

19) Poi cancellate i temporanei di Internet Explorer cercando con Pfind (o altro tool di ricerca) le cartelle di nome Content.ie5. La rimozione velocizza molto un'eventuale ulteriore scansione, con l'antivirus o l'antispymware, delle cartelle dei temporanei di Internet.

20) Poi cancellate i file sospetti nel percorso C:\WINDOWS\Downloaded Program Files (classico covo dei famigerati ActiveX malevoli).

21) Poi cancellate i file sospetti nel percorso C:\Programmi\File comuni\.

22) Poi cancellate i file sospetti nel percorso C:\WINDOWS\Cache\.

23) Poi cancellate i file sospetti nel percorso C:\WINDOWS\SHELLNEW.

24) Attenzione: negli ultimi tre punti precedenti bisogna cancellare tutti i file sospetti, ma con molta attenzione, poiché in alcune directory vi sono importanti file di sistema!

- 25) Infine, se possibile, controllate tutte le cartelle del vostro p.c., in particolare quelle in C:\, in Programmi, in Program Files e in Windows e cercate dei file che hanno nomi a noi sconosciuti o, nel nome stesso, parentesi quadre, se poi sono .exe (occhio alla doppia estensione!) ecco che sono sicuramente porcherie. Di solito si trovano collegamenti del tipo: “sesso[1].exe” o “loghiesuonerie[1].exe” o simili. Eliminare tali programmi tramite la combinazione di tasti “Maiusc + Canc” (in questo modo, il file non passerà nel Cestino e sarà cancellato direttamente).
- 26) Spesso, però, anche se il nostro antivirus o antispyware trova il file infetto, non riesce ad eliminarlo: perché?  
Semplicemente perché il file infetto, in quel momento, potrebbe essere in esecuzione, anche se invisibile ai nostri occhi, per cui non può essere eliminato se non lo si chiude prima.
- 27) Partendo dal presupposto di avere sì un malware, ma anche un Sistema Operativo sempre aggiornato ed efficiente (cioè con i Service Pack relativi) chiudete tutte le applicazioni aperte non indispensabili (esempio: chiudete Word o Winzip o il programma della stampante o della scheda audio, ma non l'antivirus o il firewall o il Systray) e lavorate esclusivamente in “Monoutenza”.
- 28) Digitare contemporaneamente “Ctrl + Alt + Canc” per poi avviare la procedura Task Manager oppure digitare dal menu “Start / Esegui...” il comando “taskmgr.exe” (ovviamente senza virgolette).
- 29) Controllare se tra i “Processi” esiste un'applicazione denominata “MSBLASTER.EXE” o altro nome “sospetto” o “sconosciuto”.
- 30) Se presente, selezionare tale applicazione, per poi forzarne la chiusura (in gergo informatico si dice “killare”) tramite il pulsante “Termina Adesso” posto in basso a destra della finestra.
- 31) Non sapete quali possono essere le applicazioni “sospette” o “sconosciute”? In effetti, dal Task Manager di Windows si vedono solo i nomi dei processi e qualche altra povera informazione, nulla in più. È il momento di avviare Autoruns (che, come detto sopra, comunque può essere degnamente sostituito da RegSeeker).
- 32) Nella schermata principale del programma, guardando nelle colonne “Description” e “Publisher”, vi viene fornita una descrizione del tipo di programma scelto e il nome del suo produttore, cose che possono essere molto utili, quando si incontrano quei virus o spyware che utilizzano un nome simile a quello di programmi regolari.
- 33) In “Image path” potete trovare il percorso (utilissimo!) da cui viene lanciato questo programma maligno.
- 34) Ora siete in grado di capire quali programmi in esecuzione sono maligni e quali no. Potete chiudere i programmi individuati. Se avete ancora dubbi, segnatevi i programmi “sospetti” e non e poi fate ripartire il vostro Sistema Operativo in modalità provvisoria (F8 all'avvio), confrontando quali programmi non sono più in esecuzione automatica.

- 35) Aprite il Registro di sistema e cancellate le chiavi sospette dai seguenti percorsi:  
HKLM\Software\Microsoft\Windows\CurrentVersion\Run  
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce  
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices  
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce  
HKCU\Software\Microsoft\Windows\CurrentVersion\Run  
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce  
Notate che HijackThis raggruppa con l'identificativo "O4" i programmi eseguiti all'avvio di Windows.
- 36) È il momento di utilizzare l'ottimo RegSeeker, programma che tra l'altro è in italiano: dopo la sua utilizzazione, esso ci segnalerà le chiavi che andrebbero rimosse (niente paura: il programma ha una funzione che permette il recupero di tali chiavi nel caso si cancellassero valori indispensabili, di default è già spuntata la casella "Ricovera" – brutto italiano, lo so... –).
- 37) Eseguire le (eventuali) procedure ("removal tool") messe a disposizione dal produttore di antivirus, che DOVREBBERO eliminare tutta la configurazione dei malware dal proprio p.c.  
Le procedure per il worm Blaster, ad esempio, possono essere recuperate dai seguenti indirizzi web: [www.pharmaservice.it/download/fixblast.exe](http://www.pharmaservice.it/download/fixblast.exe) e [www.pharmaservice.it/download/fixwelch.exe](http://www.pharmaservice.it/download/fixwelch.exe).
- 38) Raggiungere, ad esempio, la sottocartella SYSTEM32 presente nella directory WINDOWS ed eliminare il file "msblast.exe", tramite la combinazione di tasti "Maiusc + Canc".
- 39) Per sicurezza, riavviate l'antivirus o l'antispymware e scansionate di nuovo le vostre unità non removibili.
- 40) Eseguire una "patch" di Windows (XP nel nostro esempio) messa a disposizione da Microsoft, per evitare che il p.c. possa essere nuovamente infettato da QUEL TIPO di virus.  
Nell'esempio di Blaster, la patch può essere recuperata al seguente indirizzo web: [www.pharmaservice.it/download/blaster\\_xp.exe](http://www.pharmaservice.it/download/blaster_xp.exe).
- 41) Spegner il p.c. per poi riavviarlo dopo 10 / 15 secondi.
- 42) Durante la fase di spegnimento del p.c, esso potrebbe rimanere bloccato sulla finestra "Arresto del Sistema in Corso...". In tal caso premere una sola volta il pulsante di spegnimento del p.c stesso per forzare lo spegnimento.
- 43) A volte, anzi, conviene proprio riavviare il computer con "F8" in modo da partire in modalità provvisoria ed evitare che il malware venga caricato all'avvio del sistema operativo. Poi, dalla modalità provvisoria procedere alla sicura rimozione del malware stesso.
- 44) Ripetere daccapo la scansione con l'antivirus o con l'antispymware: molto difficilmente il programma troverà ancora del malware!

- 45) Riavviare RegSeeker, per rimuovere eventuali chiavi ancora legate al malware.
- 46) Ma se il programma trova ancora del malware, cosa fare?  
Beh, probabilmente lo spyware che vi siete beccati (è più semplice rimuovere un virus che uno spyware, sembra) è uno di quelli duri! E allora... facciamo i duri anche noi!
- 47) Avviate Hijackthis, cliccate su "Scan" per ottenere il report. (Piccola nota: questo programma è molto valido per quel malware che, una volta insediatosi sul sistema, introducono, per complicare la vita all'utente, addirittura delle restrizioni su sistema operativo e browser. E' possibile che l'icona delle *Opzioni Internet* sparisca dal *Pannello di controllo*, che non sia più consentito l'accesso alla finestra delle opzioni di Internet Explorer o la modifica del registro di sistema).
- 48) A questo punto, salvate il file .log cliccando su "Save log".
- 49) Se non avete dimestichezza alcuna per analizzare questo report, potete postarlo sul forum di WinTricks.it sezione Sicurezza e Privacy, o farvi una cultura qui: <http://www.help2go.com/article153.html> .  
Oppure lasciare che altri analizzino in modo automatico il vostro .log qui: <http://hijackthis.de/index.php?langselect=italian> (molto interessante e semplice da usare).
- 50) Identificati i processi e le chiavi maligne, essi possono essere spuntati e poi eliminati facendo clic su "Fix checked".
- 51) Se i file risultano in uso bisogna localizzare il task con ProcExplorer.
- 52) Chiuderli e quindi rimuoverli.  
In generale, file eseguibili, anche privi di parentesi quadre, come i succitati o altri con nomi tipo "temi.exe", "tesine.exe", "lotto.exe", "hotline.exe" sono indubbiamente dei dialers.  
In particolare, sono sicuramente degli spyware quando non vengono minimamente visualizzate informazioni chiare su di loro.  
Spesso si beccano più volte e quindi si formano cartelle con il nome "conflict.1", "conflict.2", ecc... con dentro le "porcherie".  
In caso di dubbio una veloce ricerca con un ottimo motore di ricerca spesso risolve il dubbio.
- 53) Il passo successivo è quello di utilizzare CWShredded che elimina eventuali tracce del CoolWebSearch (CWS).  
(Il pericolosissimo CoolWebSearch ci costringe ad aprire una lunga parentesi a proposito del "Default prefix hijack" di Internet Explorer. Quando si inserisce in Internet Explorer un URL non preceduto dall'identificativo del protocollo che deve essere usato (ad esempio, http://, ftp://, e così via), Windows – per default – applica il prefisso http://.  
Il prefisso predefinito può essere modificato con un semplice intervento sul registro di sistema. Alcuni malware modificano tale informazione nel registro di sistema con lo scopo di avviare i loro componenti maligni. Il diffusissimo hijacker CoolWebSearch modifica il prefisso di default sostituendolo con l'indirizzo di un sito web: in questo modo, non appena l'utente digiterà un

indirizzo nella barra degli indirizzi del browser senza anteporre <http://>, scenario certamente più comune, verrà reindirizzato sul sito web di riferimento del malware. HijackThis raggruppa i "default prefix hijack" in 013. In questi casi è bene tentare una rimozione di tutte le varianti di CoolWebSearch ad oggi conosciute usando CWShredder. Chiudiamo questa lunga parentesi)

Sempre con ProcExplorer verificare che non ci siano ancora attivi dei processi sconosciuti.

Il primo è totalmente automatico e non richiede interventi da parte dell'utente, mentre il secondo è un "task manager" molto più potente e rilascia molti dettagli sul processo (task).

Tali dettagli permettono alle volte di scovare qualcosa di sospetto anche se apparentemente risulta un elemento essenziale di Windows.

Richiede comunque un certo grado di conoscenza, non tutti i processi possono essere terminati alla leggera.

In merito a ciò consigliamo la guida di [WinTricks \(www.winticks.it\)](http://www.winticks.it) o [Google \(www.google.it\)](http://www.google.it) per attingere informazioni di riscontro ed evitare errori oppure visitare uno dei tanti siti (esempio [http://www.iamnotageek.com/a/file\\_info.php](http://www.iamnotageek.com/a/file_info.php)) per avere qualche informazione sui processi più comuni.

54) Ora è il momento di fare una pulizia profonda dei rimasugli, utilizzando il vostro abituale antispyware, ad esempio SpyBot Search & Destroy (<http://security.kolla.de/>) oppure Ad-aware (<http://www.lavasoftusa.com/>) (oppure entrambi, non vanno in conflitto, anche se il primo in ogni caso è più potente).

Ricordatevi di fare l'aggiornamento delle firme prima di procedere alla scansione.

55) Un'ulteriore passata con uno scanner on-line (tipo PestScan, qui: <http://www.pestscan.com/>) vi toglierà le briciole che tutti i precedenti software, immancabilmente, lasciano (i più refrattari ad installare software possono utilizzare questa forma di indagine e tralasciare SpyBot Search & Destroy oppure Ad-aware).

Per scrupolo o per sospetto, lanciare Stinger (che è un tool "rapido" per la rimozione dei virus più diffusi, <http://vil.nai.com/vil/stinger/>) oppure Avast Cleaner ([http://www.avast.com/eng/avast\\_cleaner.html](http://www.avast.com/eng/avast_cleaner.html), meno buono e meno veloce dello Stinger) per eliminare eventuali "compagni di ventura" dei vari trojans o virus.

56) A questo punto dovremmo avere il p.c. ragionevolmente pulito!

Non è detto che abbiamo effettivamente rimosso tutto, ma quelle poche cose che sono rimaste (forse chiavi di registro e valori alterati) non sono più in grado di nuocere ancora.

57) Per concludere il lavoro è utile proteggersi con l'uso dell'immunizzazione di SpyBot Search & Destroy, oppure utilizzare altri come [SpywareBlaster \(http://www.javacoolsoftware.com/spywareblaster.html\)](http://www.javacoolsoftware.com/spywareblaster.html).

A proposito di SpyBot Search & Destroy: è meglio utilizzare questo programma che HijackThis per i problemi relativi al Winsock.

Winsock è il driver utilizzato da Windows per effettuare transazioni di rete. Il sistema operativo lo utilizza per gestire i protocolli di rete a basso livello e le applicazioni interagiscono con Winsock per collegarsi con altri sistemi, per

comunicare con altri programmi residenti su diversi computer, per instradare dati sulla rete.

Esistono alcuni "hijackers" altamente pericolosi che, come parassiti, si "agganciano" al sistema operativo a livello di Winsock intercettando tutte le comunicazioni di rete. Si tratta di malware con la "M" maiuscola che concatenano un loro componente alle librerie Winsock di Windows: ogni volta che ci si connette ad Internet tutto il traffico passa anche attraverso i file che fanno capo all'ospite indesiderato. Il malware ha così modo di registrare, indisturbato, tutto il traffico (rubando, tra le altre cose, anche dati personali ed informazioni sensibili) e di rinviarlo a terzi.

HijackThis inserisce queste minacce nel gruppo O10 ma è altamente sconsigliabile premere il pulsante *Fix checked*: si causerebbero problemi di instabilità all'intero sistema! Per rimuovere questi componenti maligni (LSP, Layered Service Providers) è necessario servirsi dell'ultima versione di SpyBot Search & Destroy disponibile, assicurandosi di aggiornarla tramite la funzione *Cerca aggiornamenti*, *Scarica aggiornamenti* integrata nel software.

In alternativa, è possibile usare il programma LSPfix, distribuito da Cexx.org (<http://www.cexx.org/lspfix.htm>). Nel gruppo O10 di HijackThis potreste trovare componenti di software antivirus: in questo caso, non preoccupatevi assolutamente. Ciò è del tutto normale se il vostro antivirus opera a livello Winsock.

58) Infine, è il caso di procedere ad una verifica della "blindatura" del Sistema Operativo, utilizzando Windows Worms Doors Cleaner - WWDC ([http://www.sicurezzainrete.com/Windows\\_Worm\\_doors\\_clenaer.htm](http://www.sicurezzainrete.com/Windows_Worm_doors_clenaer.htm)) per chiudere tutte le porte "a rischio".

Attenzione (1): se il p.c. è in LAN non chiudete le porte 137 e 139.

Attenzione (2): i possessori del firewall Sygate Pro potrebbero incappare in un problema di corruzione risolvibile qui : <http://forums.sygate.com/vb/showthread.php?s=&threadid=1934>.

59) Un controllo on-line ci dirà se il lavoro è efficace.

Troverete diversi link alla pagina degli antivirus di WinTricks: <http://www.wintricks.it/news1/article.php?ID=1> dove sperimentare la sicurezza raggiunta.

60) Un altro trucco consiste nel proteggere dalla scrittura il file HOSTS con un semplice clic destro sul file, proprietà e poi spuntare "sola lettura".

Il file HOSTS permette di associare un indirizzo "mnemonico" (per esempio, [www.google.com](http://www.google.com)) ad uno specifico indirizzo IP. Il risultato che si ottiene ricorda da vicino quello di un comune server DNS. In Windows NT/2000/XP/2003 è presente nella cartella \SYSTEM32\DRIVERS\ETC mentre in Windows 9x/Me nella cartella d'installazione di Windows (es.: C:\WINDOWS). Molti malware o hijackers modificano il file HOSTS con lo scopo di reindirizzare il browser su siti web specifici. A seguito di questi interventi non autorizzati, digitando [www.google.com](http://www.google.com) o gli URL di altri siti web molto conosciuti, si potrebbero aprire, anziché le pagine web corrette, siti web assolutamente sconosciuti. La modifica del file HOSTS è effettuata anche da virus (un esempio è MyDoom) con lo scopo di evitare l'apertura dei siti di software house che sviluppano soluzioni antivirus.

HijackThis raggruppa con l'identificativo "01" (vedere questa pagina: <http://www.ilsoftware.it/articoli.asp?ID=2459&pag=1> ) tutti gli interventi subiti dal file HOSTS di Windows.

Tools KillHOST : <http://www.sillysot.com/other.htm> per includere determinati siti da bloccare (azione che deve essere espletata prima di mettere il file HOSTS in modalità "read only").

In relazione al file HOSTS, documentatevi su Internet come renderlo più sicuro.

### **C) COSA FARE DOPO LA RIMOZIONE**

61) Controllate anche se, nel Pannello di Controllo, la vostra connessione predefinita è rimasta quella abituale.

62) Navigare in Internet con programmi più sicuri di Microsoft Internet Explorer (esempio: installare al suo posto l'ottimo Mozilla Firefox). Oltre agli ActiveX ed ai VBScript, infatti, Internet Explorer ha anche un nemico esclusivo di nome BHO (Browser Helper Objects). Malware e spyware fanno ampio uso dei BHO. Si tratta di componenti specificamente ideati per Internet Explorer. Gli oggetti di questo tipo sono nati con lo scopo di aprire il browser Microsoft a funzionalità messe a disposizione con applicazioni sviluppate da terze parti. SpyBot Search&Destroy stesso, ad esempio, utilizza un BHO per interfacciarsi con Internet Explorer in modo da riconoscere e bloccare pagine potenzialmente pericolose. Adobe Acrobat e Google ricorrono ad oggetti BHO per dotare Internet Explorer di funzionalità per la gestione di file PDF, l'effettuazione di ricerche in Rete, l'implementazione di funzioni di "desktop search". Ma gli oggetti BHO sono ampiamente usati da malware e spyware per compiere operazioni illecite. Analoghe considerazioni possono essere fatte per le barre degli strumenti che, in sistemi poco difesi e raramente aggiornati, compaiono in massa in Internet Explorer. La presenza di BHO e barre degli strumenti maligni è evidenziabile ricorrendo all'uso di tool specifici come BHODemon (prelevabile da <http://www.ilsoftware.it/querydl.asp?ID=798> ) oppure ad HijackThis (gruppi "02" e "03": leggere questo articolo: <http://www.ilsoftware.it/articoli.asp?ID=2459> ). La loro identità può essere accertata verificando il relativo CLSID. Si tratta di un codice alfanumerico a 128 bit, scritto in esadecimale e racchiuso tra parentesi graffe. Questa pagina, <http://castleops.com/CLSID.html> , permette di consultare un ricco database contenente un vasto numero di CLSID. E' immediato verificare, ad esempio, come {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} sia un BHO legato ad Adobe Acrobat, quindi assolutamente legittimo. Infine, evitare Internet Explorer ed evitare anche siti per adulti / di suonerie gratis / di gioco d'azzardo / etc.

63) Consultare la posta elettronica con programmi più sicuri di Outlook (esempio: installare al suo posto l'ottimo Mozilla Thunderbird) ed evitare di aprire gli allegati sospetti o di abilitare la modalità "Anteprima" in un messaggio.

64) Dopo circa un mese di utilizzo del p.c. (...Ok, facciamo dopo solo una settimana, visto che siete degli utilizzatori e dei navigatori incalliti...) rimuovere i punti di ripristino precedenti e creare un nuovo punto di ripristino.

65) Poi eliminare le chiavi di registro salvate in precedenza da RegSeeker.

66) Poi cancellare la copia del backup del Registro (quella zippata con password) che avevamo fatto in precedenza.

67) Infine, fare una nuova copia del Registro di sistema, ora che è bello "pulito". Se volete, potete anche proteggere le modifiche indesiderate al Registro con due ottimi strumenti, SpywareGuard (<http://www.megalab.it/download.php?id=63> ) e RegistryProt (<http://www.megalab.it/download.php?id=64> ), il cui utilizzo è spiegato nell'articolo "Proteggere il registro di sistema" della sezione "Software applicativo" di [www.megalab.it](http://www.megalab.it) .

68) Per non beccarsi un malware la prossima volta:

- ❑ aggiornare sempre il S.O.,
- ❑ aggiornare quotidianamente le varie applicazioni riguardanti la sicurezza,
- ❑ scansionare quotidianamente il proprio p.c. con tali applicazioni,
- ❑ non disabilitare mai antivirus – antispymware – firewall - etc.,
- ❑ disabilitare la possibilità di avviare per errore potenziali virus "worm" (di solito sono un allegato ai messaggi di posta elettronica e comunque non sono altro che Visual Basic script - VBS: non appena l'utente li esegue il virus viene attivato. Uno script è una sequenza di istruzioni che possono essere utilizzate per automatizzare una serie di operazioni. L'utilizzo degli script svolge una funzione simile a quanto facevano i file batch – BAT - in MS-DOS. Chi si cura di "interpretare" tali istruzioni è il Windows Scripting Host, integrato in Windows 98 e Windows Millennium Edition. I virus di tipo "worm" utilizzano script VBS o JS per compiere operazioni maligne. In Windows Millennium, il sistema è impostato, in modo predefinito, in modo tale che gli script vengano immediatamente eseguiti non appena vi si fa doppio clic. Affinché ciò non sia possibile vi consigliamo di portarvi in Risorse del computer, scegliere dal menù "Strumenti" la voce "Opzioni cartella", fare clic sulla scheda "Tipi di file" infine eliminare dalla lista - facendo uso del pulsante "Elimina" - le seguenti associazioni: HTA, SHS, JS e VBS. In questo modo non correrete il rischio di avviare per errore potenziali virus "worm" allegati alla posta elettronica o diffusi attraverso IRC - Internet Relay Chat - .)

L'autore di questa guida ringrazia il sito

<http://home.tiscalinet.ch/winzozz/sikurezza.htm> ed il libro "L'acchiappavirus" di Paolo Attivissimo (<http://www.attivissimo.net/> ) per i preziosi consigli.

Questa guida è stata scritta da un semplice appassionato di informatica, che si è fatto (tanta) esperienza con i (tanti) p.c. infettati dei suoi amici, che avevano TUTTI qualcosa in comune: antivirus (famoso ma piratato) scaduto, scansioni del sistema con l'antivirus rare, nessun firewall, nessun anti-spyware, browser predefinito Internet Explorer....

... A voi le debite conclusioni!